United States Government Accountability Office

GAO

Testimony

Before the Subcommittee on Oversight, Investigations, and Management; Committee on Homeland Security; House of Representatives

For Release on Delivery
Expected at 10:00 a.m. CDT
Wednesday, August 24, 2011

MARITIME SECURITY

Progress Made, but Further Actions Needed to Secure the Maritime Energy Supply

Statement of Stephen L. Caldwell, Director
Homeland Security and Justice Issues

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
24 AUG 2011		**00-00-2011 to 00-00-2011**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Maritime Security: Progress Made, but Further Actions Needed to Secure the Maritime Energy Supply	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Government Accountability Office,441 G Street NW,Washington,DC,20548**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**28**	

August 24, 2011

MARITIME SECURITY

Progress Made, but Further Actions Needed to Secure the Maritime Energy Supply

GAO Accountability * Integrity * Reliability

Highlights

Highlights of GAO-11-883T, a testimony before the Subcommittee on Oversight, Investigations, and Management; Committee on Homeland Security; House of Representatives

Why GAO Did This Study

The nation's economy and security are heavily dependent on oil, natural gas, and other energy commodities. Al-Qa'ida and other groups with malevolent intent have targeted energy tankers and offshore energy infrastructure because of their importance to the nation's economy and national security. The U.S. Coast Guard—a component of the Department of Homeland Security (DHS)—is the lead federal agency for maritime security, including the security of energy tankers and offshore energy infrastructure. The Federal Bureau of Investigation (FBI) also has responsibilities for preventing and responding to terrorist incidents. This testimony discusses the extent to which (1) the Coast Guard and the FBI have taken actions to address GAO's prior recommendations to prevent and respond to a terrorist incident involving energy tankers and (2) the Coast Guard has taken actions to assess the security risks to offshore energy infrastructure and related challenges. This testimony is based on products issued from December 2007 through March 2011 and recently completed work on the Coast Guard's actions to assess security risks. GAO reviewed documents from the Coast Guard's risk model and relevant laws, regulations, policies, and procedures; and interviewed Coast Guard officials.

What GAO Recommends

GAO is recommending that the Coast Guard revise policies and procedures to ensure its analysts receive the annual updated list of regulated offshore energy facilities to ensure risk assessments are conducted on those facilities. The Coast Guard concurred with this recommendation.

View GAO-11-883T or key components. For more information, contact Stephen Caldwell at (202) 512-9610 or caldwells@gao.gov.

What GAO Found

The Coast Guard and the FBI have made progress implementing prior recommendations GAO made to enhance energy tanker security. In 2007, GAO made five recommendations to address challenges in ensuring the effectiveness of federal agencies' actions to protect energy tankers and implement response plans. The Coast Guard and the FBI have implemented two recommendations, specifically: (1) the Coast Guard, in coordination with U.S. Customs and Border Protection, developed protocols for facilitating the recovery and resumption of trade following a disruption to the maritime transportation system, and (2) the Coast Guard and the FBI participated in local port exercises that executed multiple response plans simultaneously. The Coast Guard has made progress on a third recommendation through work on a national strategy for the security of certain dangerous cargoes. It also plans to develop a resource allocation plan, starting in April 2012, which may help address the need to balance security responsibilities. However, the Coast Guard and the FBI have not yet taken action on a fourth recommendation to develop an operational plan to integrate the national spill and terrorism response plans. According to DHS, it plans to revise the *National Response Framework*, but no decision has been made regarding whether the separate response plans will be integrated. Also, DHS has not yet taken action on the final recommendation to develop explicit performance measures for emergency response capabilities and use them in risk-based analyses to set priorities for acquiring needed response resources. According to DHS, it is revising its emergency response grant programs, but does not have specific plans to develop performance measures as part of this effort.

The Coast Guard has taken actions to assess the security risks to offshore energy infrastructure, which includes Outer Continental Shelf (OCS) facilities (facilities that are involved in producing oil or natural gas) and deepwater ports (facilities used to transfer oil and natural gas from tankers to shore), but improvements are needed. The Coast Guard has used its Maritime Security Risk Analysis Model (MSRAM) to examine the security risks to OCS facilities and deepwater ports. To do so, the Coast Guard has coordinated with the intelligence community and stakeholders, such as the Department of the Interior's Bureau of Ocean Energy Management, Regulation and Enforcement. However, the Coast Guard faces complex and technical challenges in assessing risks. For example, the Coast Guard does not have data on the ability of an OCS facility to withstand an attack. The Coast Guard generally recognizes these challenges and has actions underway to study or address them. Further, GAO determined that as of May 2011, the Coast Guard had not assessed security risks for 12 of the 50 security-regulated OCS facilities that are to be subjected to such assessments. Coast Guard officials later determined that they needed to add these OCS facilities to MSRAM for assessment and have completed the required assessments. However, while the list of security-regulated facilities may change each year based on factors such as production volume, the Coast Guard's current policies and procedures do not call for Coast Guard officials to provide an annual updated list of regulated OCS facilities to MSRAM analysts. Given the continuing threat to such offshore facilities, revising its procedures could help ensure that the Coast Guard carries out its risk assessment requirements for security-regulated OCS facilities.

Chairman McCaul, Ranking Member Keating, and Members of the Subcommittee:

I am pleased to be here today to discuss federal efforts to ensure the security of energy tankers and the offshore energy infrastructure that produces, transports, or receives oil and natural gas. The nation's economy and security are heavily dependent on oil, natural gas, and other energy commodities. Further, it is fitting that today's hearing is in Houston because the city and the surrounding area play a central role in the maritime energy sector. Houston is home to hundreds of energy companies and many of these companies are involved in exploring for and producing oil and natural gas in the Gulf of Mexico and transporting it from sea to shore. In addition, energy tankers sail through the Houston Ship Channel, and major facilities for refining oil are located along or near the channel.

Al-Qa'ida and other groups with malevolent intent continue to target energy tankers and offshore energy infrastructure because of their importance to the nation's economy and national security. In May 2011, the Department of Homeland Security (DHS) issued a press statement that intelligence information showed that throughout 2010 there was continuing interest by members of al-Qa'ida in targeting oil tankers and commercial oil infrastructure at sea. While a terrorist attack on energy tankers or offshore energy infrastructure has not occurred in the United States, other countries have experienced such attacks.

Additionally, while it was not the result of an attack, the *Deepwater Horizon* explosion in April 2010 showed that the consequences of an incident on offshore energy infrastructure could be significant. The explosion resulted in 11 deaths, serious injuries, and the largest oil spill in the history of the United States. The response to the incident encountered numerous challenges, and by the time the well was sealed nearly 3 months later, over 4 million barrels of oil had spilled into the Gulf. The spill created significant environmental damage and had an adverse impact on workers and businesses, with an estimated cost to compensate for these damages totaling billions of dollars.

The U.S. Coast Guard—a component of DHS—is the lead federal agency for maritime security, including security of energy tankers and offshore energy infrastructure. The FBI—an agency in the Department of Justice (DOJ)—shares responsibility with the Coast Guard for preventing and responding to terrorist incidents in the maritime environment, including incidents involving energy tankers. In December 2007, we issued a report

that examined Coast Guard and FBI efforts to prevent and respond to an incident involving energy tankers and we made several recommendations to the Coast Guard and the FBI to improve efforts in these areas.[1]

My testimony today will address two main objectives:

- the extent to which the Coast Guard and the FBI have taken actions to address our prior recommendations to prevent and respond to terrorist incidents involving energy tankers, and
- the extent to which the Coast Guard has taken actions to assess the security risks to offshore energy infrastructure and the challenges, if any, in conducting such assessments.

My statement is based on our past work on energy tankers issued in December 2007 and recently completed work on actions the Coast Guard has taken to assess security risks in the maritime environment.[2] To obtain information on the first objective, we reviewed our prior reports on energy tankers, and asked the Coast Guard and the FBI to provide us an update, along with supporting documentation, on any actions that they have taken to address our recommendations from the December 2007 report. To provide additional information on threats to energy tankers, we also reviewed our recent work on piracy.[3] More detailed information on the scope and methodology used for our past reviews appears in those reports.

To address the second objective, we interviewed officials in Coast Guard headquarters and field offices in New Orleans, Louisiana and Boston, Massachusetts because these officials were knowledgeable about how the Coast Guard uses the Maritime Security Risk Analysis Model (MSRAM)—a tool that the Coast Guard uses to assess the security risks

[1]GAO, *Maritime Security: Federal Efforts Needed to Address Challenges in Preventing and Responding to Terrorist Attacks on Energy Commodity Tankers*, GAO-08-141 (Washington, D.C.: Dec. 10, 2007).

[2]GAO-08-141.

[3]GAO, *Maritime Security: Actions Needed to Assess and Update Plan And Enhance Collaboration among Partners Involved in Countering Piracy off the Horn of Africa*, GAO-10-856 (Washington, D.C.: Sept. 24, 2010); and *Maritime Security: Updating U.S. Counterpiracy* Action Plan *Gains Urgency as Piracy Escalates off the Horn of Africa*, GAO-11-449T (Washington, D.C.: Mar. 15, 2011).

to vessels and offshore energy infrastructure.[4] Moreover, the New Orleans and Boston field offices are the only offices presently conducting assessments of offshore energy infrastructure. We also reviewed Coast Guard documents on MSRAM, such as Coast Guard guidance to its field units and the MSRAM training manual. In addition, we reviewed relevant laws and regulations, policies and procedures, and other documents related to security risk assessments. For example, we reviewed the DHS Quadrennial Review,[5] the National Infrastructure Protection Plan,[6] and a National Research Council report on risk assessments at DHS.[7] We also reviewed our prior report on risk assessment efforts carried out by the Coast Guard.[8] In addition, we compared the Coast Guard's policies and procedures regarding security actions with criteria in *Standards for*

[4]In looking at the Coast Guard's assessments of risks, we focused on security risks—risks emanating from terrorists or others that would purposely attack or sabotage offshore energy infrastructure. We did not focus on accidental risks to such infrastructure. However, we have ongoing work to assess industry plans for developing new methods or technologies to control and contain blowouts occurring in subsea environments. We are conducting this work at the request of the Ranking Member of the House Committee on Energy and Commerce. We expect to issue this related report in the winter of 2012. We are also conducting broader work examining the Coast Guard's use of MSRAM for the Chairman of the Senate Committee on Commerce, Science, and Transportation; the Ranking Member of the Senate Committee on Homeland Security and Governmental Affairs; and the Chairwoman of the House Homeland Security Committee, Subcommittee on Border and Maritime Security. We expect to issue this report later in 2011.

[5]The DHS Quadrennial Review outlines a strategic framework for stakeholders, including federal, state, local, tribal, territorial, nongovernmental, and private-sector entities, in responding to security threats. For more information about the DHS Quadrennial Review, see GAO, *Quadrennial Homeland Security Review: 2010 Reports Addressed Many Required Elements, but Budget Planning Not Yet Completed*, GAO-11-153R (Washington, D.C.: Dec. 16, 2010).

[6]The National Infrastructure Protection Plan represents a strategy for protecting critical infrastructure and key resources, and it offers a framework for assessing risk. For more information about the National Infrastructure Protection Plan, see GAO, *Critical Infrastructure Protection: Update to National Infrastructure Protection Plan Includes Increased Emphasis on Risk Management and Resilience*, GAO-10-296 (Washington, D.C.: Mar. 5, 2010).

[7]National Research Council: *Review of the Department of Homeland Security's Approach to Risk Analysis* (Washington, D.C.: 2010).

[8]GAO, *Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure,* GAO-06-91 (Washington, D.C.: Dec. 15, 2005) and *Maritime Security: DHS Progress and Challenges in Key Areas of Port Security*, GAO-10-940T (Washington, D.C.: July 21, 2010).

Internal Control in the Federal Government.[9] Further, we interviewed representatives from two companies that together operate 18 of the 50 Outer Continental Shelf facilities, a type of offshore energy infrastructure, regulated for security in 2011. While the information obtained from these interviews is not generalizable to the offshore energy industry as a whole, it provided insights into owners' and operators' concerns regarding security and actions they have taken to address such concerns. This testimony concludes our work on Coast Guard efforts to assess security risks for offshore energy infrastructure.[10]

We conducted this performance audit from October 2010 through August 2011 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

The nation's economy and security are heavily dependent on oil, natural gas, and other energy commodities. Nearly half of the nation's oil is transported from overseas by tankers. For example, about 49 percent of the nation's crude oil supply—one of the main sources of gasoline, jet fuel, heating oil, and many other petroleum products—was transported by tanker into the United States in 2009.[11] The remaining oil and natural gas used in the United States comes from Canada by pipeline or is produced from domestic sources in areas such as offshore facilities in the Gulf of Mexico. With regard to these domestic sources, the area of federal jurisdiction—called the Outer Continental Shelf (OCS)[12]—contains an estimated 85 million barrels of oil, more than all onshore resources and

[9]GAO, *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: November 1999).

[10]We will continue our broader work looking at the security of offshore energy infrastructure, including Coast Guard security inspections and other challenges.

[11]This figure is based on the most recently available data for a full year from the U.S. Energy Information Administration.

[12]The OCS is a designation for all submerged lands of which the subsoil and seabed are outside the territorial jurisdiction of a U.S. state, but within U.S. jurisdiction and control.

those in shallower state waters combined.[13] In addition, the Louisiana Offshore Oil Port (LOOP), a deepwater port, is responsible for transporting about 10 percent of imported oil into the United States.

Federal Agency Roles

As the lead federal agency for maritime security, the Coast Guard seeks to mitigate many kinds of security challenges in the maritime environment. Doing so is a key part of its overall security mission and a starting point for identifying security gaps and taking actions to address them. Carrying out these responsibilities is a difficult and challenging task because energy tankers often depart from foreign ports and are registered in countries other than the United States, which means the United States has limited authority to oversee the security of such vessels until they enter U.S. waters. Offshore energy infrastructure also presents its own set of security challenges because some of this infrastructure is located many miles from shore. The FBI shares responsibility with the Coast Guard for preventing and responding to terrorist incidents in the maritime environment, including incidents involving energy tankers.

Risks to Energy Tankers

Energy tankers face risks from various types of attack. We identified three primary types of attack methods against energy tankers in our 2007 report, including suicide attacks, armed assaults by terrorists or armed bands, and launching a "standoff" missile attack using a rocket or some other weapon fired from a distance. In recent years, we have issued reports that discussed risks energy tankers face from terrorist attacks and attacks from other criminals, such as pirates. Terrorists have attempted—and in some cases carried out—attacks on energy tankers since September 11, 2001. To date, these attacks have included attempts to damage tankers or their related infrastructure at overseas ports. For example, in 2002, terrorists conducted a suicide boat attack against the French supertanker *Limburg* off the coast of Yemen, and in 2010, an incident involving another supertanker, the *M/V M. Star*, in the Strait of Hormuz is suspected to have been a terrorist attack. Our work on energy tankers identified three main places in which tankers may be at risk of an attack: (1) at foreign ports; (2) in transit, especially at narrow channels, or chokepoints; and (3) at U.S. ports. For example, foreign ports, where

[13]Based on an estimate from the National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling, *Deep Water: The Gulf Oil Disaster and the Future of Offshore Drilling* (Washington, D.C.: January 2011).

commodities are loaded onto tankers, may vary in their levels of security, and the Coast Guard is limited in the degree to which it can bring about improvements abroad when security is substandard, in part because its activities are limited by conditions set by host nations. In addition, while tankers are in transit, they face risks because they travel on direct routes that are known in advance and, for part of their journey, they may have to travel through waters that do not allow them to maneuver away from possible attacks. According to the Energy Information Administration, chokepoints along a route make tankers susceptible to attacks. Further, tankers remain at risk upon arrival in the United States because of the inherent risks to port facilities. For example, port facilities are generally accessible by land and sea and are sprawling installations often close to population centers.

Beyond the relatively rare threat of terrorist attacks against tankers, the threat of piracy has become relatively common.[14] In particular, piracy threatens tankers transiting one of the world's busiest shipping lanes near key energy corridors and the route through the Suez Canal. The vast areas at risk for piracy off the Horn of Africa, combined with the small number of military ships available for patrolling them, make protecting energy tankers difficult. According to the International Maritime Bureau, 30 percent (490 of 1,650) of vessels reporting pirate attacks worldwide from 2006 through 2010 were identified as tankers.[15] See table 1 for a summary of tankers attacked by pirates during 2006 through 2010.

[14]The motivation behind an attack may distinguish piracy from terrorism. For example, the motivation for piracy is often monetary, whereas terrorism is politically motivated.

[15]The International Chamber of Commerce's International Maritime Bureau operates a Piracy Reporting Center that collects data on pirate attacks worldwide.

Table 1: Number of Tankers Attacked by Pirates, 2006 – 2010

Type of commodity transported	2006	2007	2008	2009	2010
Bitumen[a]		1		2	2
Chemical/Product[b]	35	52	55	69	96
Crude Oil	9	25	30	41	43
Liquefied Natural Gas		1		1	1
Liquefied Petroleum Gas	4	5	6	5	7
Totals	**48**	**84**	**91**	**118**	**149**

Source: International Maritime Bureau, *Piracy and Armed Robbery Against Ships Annual Report* (United Kingdom, 2010)

[a]Bitumen is a heavy black viscous oil often used in paving materials and sealants.

[b]This category includes tankers that transport chemicals or oil products other than crude oil.

As shown in the table, pirate attacks against tankers have tripled in the last 5 years, and the incidence of piracy against tankers continues to rise. From January through June 2011, 100 tankers were attacked, an increase of 37 percent compared to tankers attacked from January through June 2010. Figure 1 shows one of the recent suspected pirate attacks. In addition, tankers are fetching increasing ransom demands from Somali pirates. Media reports indicate a steady increase in ransoms for tankers, from $3 million in January 2009 for the Saudi tanker *Sirius Star*, to $9.5 million in November 2010 for the South Korean tanker *Samho Dream*, to $12 million in June 2011 for the Kuwaiti tanker *MV Zirku*. The U.S. Maritime Administration and the Coast Guard have issued guidance for commercial vessels to stay 200 miles away from the Somali coast. However, pirates have adapted and increased their capability to attack and hijack vessels to more than 1,000 miles from Somalia using mother ships, from which they launch smaller boats to conduct the attacks.[16] To address the growing concern over piracy, the Coast Guard has issued a directive with guidelines for U.S. vessels operating in high-risk waters. This directive provides vessel owners and operators with direction for responding to emerging security risks.

[16]For more information on U.S. government efforts to combat piracy, see GAO-10-856, which discusses the Coast Guard's and other agencies' progress in implementing efforts to prevent piracy attacks. This report contains recommendations to improve U.S. government efforts to combat piracy.

Figure 1: Sailors from the U.S. Navy's *USS Philippine Sea* Rescue Crew of the Tanker *VLCC Brilliante Virtuoso* in Response to a Suspected Attack by Pirates, June 2011

Source: U.S. Navy.

Risks to Offshore Energy Infrastructure

Offshore energy infrastructure also faces risks from various types of attacks. For example, in 2004, a terrorist attacked an offshore oil terminal in Iraq using speedboats packed with explosives, killing two U.S. Navy sailors and a U.S. Coast Guardsman. Potential attack methods against offshore energy infrastructure identified by the Coast Guard or owners and operators include crashing an aircraft into it; using a submarine vessel, diver, or other means of attacking it underwater; ramming it with a vessel; and sabotage by an employee. Offshore energy infrastructure may face security risks because this infrastructure is located in open waters and generally many miles away from Coast Guard assets and personnel.

In addition to our work on energy tankers, we have recently completed work involving Coast Guard efforts to assess security risks and ensure the security of offshore energy infrastructure. Specifically, our work focused on two main types of offshore energy infrastructure that the

Coast Guard oversees for security. The first type are facilities that operate on the OCS and are generally described as facilities temporarily or permanently attached to the subsoil or seabed of the OCS that engage in exploration, development, or production of oil, natural gas, or mineral resources.[17] As of September 2010, there were about 3,900 such facilities, and if a facility of this type meets or exceeds any one of three thresholds for production or personnel, it is subject to 33 C.F.R. part 106 security requirements.[18] In this testimony, we focus on the 50 facilities that, in 2011, are regulated for security because they meet or exceed the threshold criteria. We refer to these security-regulated facilities as OCS facilities. The second type of offshore energy infrastructure are deepwater ports, which are fixed or floating manmade structures used or intended for use as a port or terminal for the transportation, storage, or handling of oil or natural gas to any state and includes the transportation of oil or natural gas from the United States' OCS.[19] There are currently four licensed deepwater ports—two in the Gulf of Mexico and two in Massachusetts Bay.[20] Unlike OCS facilities, which are involved in the production of oil or natural gas, deepwater ports enable tankers to offload oil or liquefied natural gas for transport to land by underwater pipelines.

[17]See 33 C.F.R. § 106.105.

[18]Facilities meeting any of the threshold criteria are often referred to as Maritime Transportation and Security Act (MTSA)-regulated facilities. The production or personnel thresholds for determining whether an OCS facility will be subject to security requirements in accordance with 33 C.F.R. part 106 are: (1) producing greater than 100,000 barrels of oil a day, (2) producing more than 200 million cubic feet of natural gas per day, or (3) hosting more than 150 persons for 12 hours or more in each 24 hour period continuously for 30 days or more. According to 33 C.F.R. § 140.10, production means those activities which take place after the successful completion of any means for the removal of minerals, including, but not limited to, such removal, field operations, transfer of minerals to shore, operation monitoring, maintenance, and workover. According to the Coast Guard, the statement; "transfer of minerals to shore" encompasses fixed facilities that operate as "Transmission Facilities." Production quantities shall be calculated as the sum of all sources of production from wells on the primary and any attending platform(s), including the throughput of other pipelines transferring product across the same platform(s).

[19]See 33 C.F.R. § 148.5. Although deepwater ports are generally not regulated for security in accordance with MTSA, owners and operators generally carry out similar measures to those carried out for OCS facilities by, among other things, developing security plans comparable to those implemented by OCS facilities pursuant to part 106. See 33 C.F.R. § 150.15(x).

[20]According to the Coast Guard, one of the Gulf of Mexico deepwater ports is expected to be decommissioned in the near future.

Progress Made Addressing Our Recommendations, but Additional Actions Could Help Improve Tanker Security

In 2007, we assessed Coast Guard and FBI efforts to ensure the security of energy tankers and respond to terrorist incidents involving energy tankers.[21] We found that actions were being taken, internationally and domestically, to protect tankers and port facilities at which tankers would be present. For example, the Coast Guard visits foreign exporting ports to assess the effectiveness of the anti-terrorism measures in place. Additionally, port stakeholders in the United States have taken steps to address vulnerabilities at domestic ports. For example, the Houston Ship Channel Security District is a public-private partnership that was established to increase preparedness and response capabilities with the goal of improving security and safety for facilities, employees, and communities surrounding the Houston Ship Channel. The security district has installed technology, such as night vision and motion-activated detection equipment, and conducts patrols on land and in the water. However, we also reported on challenges that remained in (1) making federal agencies' protective actions more effective and (2) implementing plans for a response to an attack, if a terrorist attack were to succeed despite the protective measures in place.

We made five recommendations in our 2007 report, three of which were directed to the Secretary of Homeland Security and two of which were directed jointly to the Secretary of Homeland Security and the Attorney General. The departments concurred or partially concurred with all of the recommendations. The Coast Guard and the FBI have made progress in implementing these recommendations—two have been implemented, and the Coast Guard is in the process of implementing a third—but actions have not yet been taken to address the remaining two recommendations. See table 2 for a summary of our findings, recommendations, and the current status of agency efforts to implement our recommendations.

[21] GAO-08-141.

Table 2: Status of GAO Recommendations on Tanker Security from GAO-08-141

Findings	Recommendation and Status
Resource allocation. Based on Coast Guard records, we found that Coast Guard field units in several energy-related ports had been unable to accomplish many of the port security responsibilities called for in Coast Guard guidance. According to the data we obtained and our discussions with field unit officials, we determined that resource shortfalls were the primary reasons for not meeting these responsibilities. Furthermore, the Coast Guard had not yet developed a plan for addressing new liquefied natural gas (LNG) security resource demands.	**Recommendation.** We recommended that the Coast Guard develop a national resource allocation plan that would balance the need to meet new LNG security responsibilities with existing security responsibilities and other Coast Guard missions. **Status – In progress.** The Coast Guard has begun work on a national strategy for reducing the maritime security risks present in the bulk transportation and transfer of certain dangerous cargoes, including LNG. Coast Guard officials expect to finalize the strategy in April 2012 at which point they expect to develop a resource allocation plan to implement the strategy. In the interim, the Coast Guard has published guidance to clarify the timing and scope of the process that is necessary to ensure full consideration is given to safety and security of the port, the facility, and the vessels transporting LNG.
Guidance for helping to mitigate economic consequences. We reported that the economic consequences of a terrorist attack on a tanker could be significant, particularly if one or more ports are closed. We identified some ports that, on their own initiative, were incorporating economic recovery considerations into their port-level plans, but at the time of our review in 2007, there was no national-level guidance for use by local ports.	**Recommendation.** We recommended that the Coast Guard develop guidance that ports could use to plan for helping to mitigate economic consequences, particularly in the case of port closures. **Status – Implemented.** The Coast Guard and U.S. Customs and Border Protection (CBP) have developed Joint Protocols for the Expeditious Recovery of Trade. These protocols establish a communications process and describe how the Coast Guard and CBP will coordinate with other federal agencies and the maritime industry to facilitate recovery and resumption of trade following an event that causes a major disruption to the maritime transportation system.
Integration of spill and terrorism response at the national level. We found that while national- and port-level plans exist to address spill response or terrorism response, federal agencies and ports could face challenges in using them effectively. We reported that the separate spill and terrorism response plans should be integrated for responding to an attack on an energy commodities tanker.	**Recommendation.** We recommended that the Coast Guard and the FBI coordinate at the national level to help ensure that a detailed operational plan be developed that integrates the different spill and terrorism sections of the *National Response Plan*. **Status – Not implemented.** The different spill and terrorism response sections of the *National Response Plan* remain separate annexes in the renamed *National Response Framework*. According to the Coast Guard, the *National Response Framework* is currently under revision, but no decision has been made regarding the spill and terrorism response annexes. Pending that decision, the FBI has not taken any action to implement this recommendation.
Integration of spill and terrorism response at the local level. In addition to the need for operational plans as noted above, we reported that agencies should conduct joint exercises that simulate an attack and the agencies' responses. Without such exercises, it would be questionable whether joint Coast Guard and FBI activities would proceed as planned.	**Recommendation.** We recommended that the Coast Guard and FBI coordinate at the local level to help ensure that spill and terrorism response activities are integrated for the best possible response by maximizing the integration of spill and terrorism response planning and exercises at ports that receive energy commodities where attacks on tankers pose a significant threat. **Status – Implemented.** In April 2008, the Coast Guard updated guidance which states that the ability to simultaneously execute multiple plans, including federal, state, and local response and recovery plans, should be part of an overall exercise and preparedness program. In accordance with this guidance, the Coast Guard, along with the FBI and other stakeholders, has conducted exercises that address an integrated spill and terrorism response.

Findings	Recommendation and Status
Performance measures for emergency response. We found that some ports had reported difficulty in securing response resources to carry out planned actions and decisions about the need for more response capabilities were hindered by a lack of performance measures tying resource needs to effectiveness in response.	**Recommendation.** We recommended that the Secretary of Homeland Security work with federal, state, and local stakeholders to develop explicit performance measures for emergency response capabilities and use them in risk-based analyses to set priorities for acquiring needed response resources. **Status – Not implemented.** DHS has not yet developed explicit performance measures for emergency response capabilities. According to DHS, it is revising its grant programs, but performance measures have not yet been developed as part of this effort.

Source: GAO.

Regarding our recommendation that the Coast Guard and the FBI coordinate to help ensure that a detailed operational plan be developed that integrates the different spill and terrorism sections of the *National Response Framework*, DHS is in the process of revising this document and did not have further information regarding whether or how the spill and terrorism response annexes may be revised. Further, the FBI has not taken independent action to implement this recommendation, in part because it did not concur with the need to develop a separate operational plan. In the event of a successful attack on an energy tanker, ports would need to provide an effective, integrated response to (1) protect public safety and the environment, (2) conduct an investigation, and (3) restore shipping operations in a timely manner. Consequently, clearly defined and understood roles and responsibilities for all essential stakeholders are needed to ensure an effective response, and operational plans for the response should be explicitly linked. Regarding our recommendation that DHS develop performance measures for emergency response capabilities, DHS has begun to revise its grant programs, but it is too early in that process to determine whether and how performance measures will be incorporated into those revisions. Performance measures would allow DHS to set priorities for funding on the basis of reducing overall risk, thereby helping ports obtain resources necessary to respond. We continue to believe that the recommendations not yet addressed have merit and should be fully implemented.

Coast Guard Had Not Assessed Risks to All OCS Facilities

In accordance with federal statutes and presidential directives, the Coast Guard assesses security risks as part of its responsibilities for ensuring the security of OCS facilities and deepwater ports. In doing so, the Coast Guard, among other things, uses a tool called the Maritime Security Risk Analysis Model (MSRAM). Coast Guard units throughout the country use this tool to assess security risks to about 28,000 key infrastructure in and around the nation's ports and waterways. For example, MSRAM

examines security risks to national monuments, bridges, and oil and gas terminals.

The Coast Guard's efforts to assess security risks to OCS facilities and deepwater ports are part of a broader effort by DHS to protect critical infrastructure and key resources.[22] To further guide this effort, in 2009 DHS issued an updated version of the 2006 National Infrastructure Protection Plan which describes the department's strategic approach to infrastructure protection.[23] The plan placed an increased emphasis on risk management and it centered attention on going beyond assessments of individual assets by extending the scope of risk assessments to systems or networks.[24] For example, while the 2006 plan focused on assessing the vulnerability of facilities, the 2009 plan discussed efforts to conduct systemwide vulnerability assessments.

Progress Made Assessing Offshore Security Risks

The Coast Guard has taken a number of actions in assessing security risks to OCS facilities and deepwater ports. The Coast Guard has used MSRAM to, among other things, examine security risks to OCS facilities and deepwater ports by assessing three main factors—threats,

[22]The Homeland Security Act of 2002, enacted the same day as MTSA (November 25, 2002), established DHS and gave the department wide-ranging responsibilities for, among other things, leading and coordinating the overall national critical infrastructure protection effort. Title II of the Homeland Security Act, as amended, primarily addresses the department's responsibilities for critical infrastructure protection. According to DHS, there are thousands of facilities in the United States that if degraded or destroyed by a manmade or natural disaster could cause some combination of significant casualties, major economic losses, or widespread and long-term disruptions to national well-being and governance capacity.

[23]DHS, *National Infrastructure Protection Plan, Partnering to Enhance Protection and Resiliency* (Washington, D.C: January 2009). This plan represents a strategy for protecting critical infrastructure and key resources and it offers a framework for assessing risk. DHS issued the original plan in June 2006.

[24]Network effects involve the ripple effect of an incident or simultaneous incidents on key sectors of the economy. For example, production facilities, pipelines, transfer stations, and refineries are part of the oil and natural gas network in and around the Gulf of New Mexico. Assessing network effects could involve determining whether a terrorist attack on a few key assets would have a disproportionate effect on the performance of this network. Such an assessment could examine the degree to which such an incident could disrupt the flow of oil or natural gas to industries that use these types of energy as inputs to their production functions.

vulnerabilities, and consequences.[25] First, Coast Guard analysts use MSRAM to assess security risks against such energy infrastructure by examining potential scenarios terrorists may use to attack OCS facilities or deepwater ports. For example, MSRAM assesses attack scenarios, such as an attack by a hijacked vessel, a small boat attack, sabotage, or an attack by a swimmer or diver. Second, the analysts use MSRAM to evaluate vulnerabilities of OCS facilities and deepwater ports by examining the probability of a successful attack by assessing factors such as the ability of key stakeholders, including the owner, operator, or law enforcement, to interdict an attack and the ability of a target to withstand an attack. Third, the analysts use MSRAM to evaluate potential consequences of an attack, such as deaths or injuries and economic and environmental impacts.[26] MSRAM's output produces a risk index number for each maritime target—such as an OCS facility or deepwater port—that allows Coast Guard officials at the local, regional, and national levels to compare and rank critical infrastructure for the purpose of informing security decisions. According to Coast Guard officials, based on MSRAM's output, which is a relative risk ranking, OCS facilities are not considered to be high-risk targets.

To inform analysts' inputs into MSRAM, the Coast Guard has coordinated efforts with the intelligence community and key stakeholders. For example, the Coast Guard's Intelligence Coordination Center inputs threat assessment data into MSRAM. Coast Guard analysts also use

[25]DHS defines threat as a natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property. For the purpose of calculating risk, the threat of an intentional hazard is generally estimated as the likelihood of an attack being attempted by an adversary; for other hazards, threat is generally estimated as the likelihood that a hazard will manifest itself. In the case of terrorist attacks, the threat likelihood is estimated based on the intent and capability of the adversary. DHS defines vulnerability as a physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard. In calculating the risk of an intentional hazard, a measure of vulnerability is the likelihood that an attack is successful, given that it is attempted. DHS defines consequence as the effect of an event, incident, or occurrence; reflects the level, duration, and nature of the loss resulting from the incident. For the purposes of the National Infrastructure Protection Plan, consequences are divided into four main categories: public health and safety (i.e., loss of life and illness); economic (direct and indirect); psychological; and governance/mission impacts.

[26]MSRAM assesses consequences of six factors: (1) deaths and injuries, (2) primary economic impact, (3) environmental impact, (4) national security impacts, (5) symbolic impacts, and (6) secondary economic impacts.

information from other stakeholders, such as reports produced by the Department of the Interior's Bureau of Ocean Energy Management, Regulation and Enforcement (BOEMRE), which contain oil and gas production data, to inform their evaluations of vulnerabilities and consequences. Based on the assessments of threats, vulnerabilities, and consequences, MSRAM produces a risk index number for each OCS facility and deepwater port. The Coast Guard has also taken actions to supplement MSRAM by, among other things, (1) including new data fields on the frequency with which tankers visit a port and (2) adding additional threat scenarios, such as a threat involving a cyber attack, to its data set.

While MSRAM has been applied to deepwater ports, Coast Guard officials have also used an independent risk assessment to assess security risks as part of the application process for recently constructed deepwater ports. For example, in December 2006, as part of the application process for a proposed deepwater port in the Massachusetts Bay, the Coast Guard, the owner and operator, and other stakeholders collectively identified and assessed threat scenarios as well as the potential consequences and vulnerabilities of each scenario. Based on this assessment, stakeholders identified and agreed to carry out security measures to mitigate the risks, such as installing camera systems and increasing radar coverage.

Challenges in Data and Scope Hinder Risk Assessments

The Coast Guard faces complex and technical challenges in assessing security risks. The Coast Guard recognizes these challenges and generally has actions underway to study or address them. Coast Guard officials noted that some of these challenges are not unique to the Coast Guard's risk assessment model and that these challenges are faced by others in the homeland security community involved in conducting risk assessments. Specific challenges are detailed below.

Challenges in Data

- **Vulnerability-related data:** The Coast Guard does not have data on the ability of an OCS facility to withstand an attack, which is defined in MSRAM as target hardness. The Coast Guard recognizes that target hardness is an important consideration in assessing the vulnerability of OCS facilities. However, MSRAM analysts described challenges in assessing target hardness because empirical data are not available or research has not been conducted to do so. For example, research on whether a hijacked boat or an underwater attack could sink an offshore oil or natural gas platform would give the Coast Guard and

owners and operators a clearer sense of whether this attack scenario could result in major consequences. Coast Guard officials and corporate security officers with whom we spoke indicated that such research would advance knowledge about the vulnerabilities of OCS facilities and deepwater ports. Gaining a better understanding of target hardness of these and other threat scenarios could improve the quality of the output from MSRAM. According to Coast Guard's MSRAM Program Manager, the Coast Guard may recommend conducting more research on the vulnerability to and consequences of attack scenarios as a result of a study it is currently conducting on OCS facilities in the Gulf of Mexico. The Coast Guard initiated this study in the fall of 2010 after the *Deepwater Horizon* incident. The study initially reviewed the "lessons learned" from *Deepwater Horizon* and how those lessons could be used to improve MSRAM. During the course of our review, Coast Guard officials stated that the scope of the study has been expanded to include OCS facilities and that the Coast Guard expects to issue its report in the fall of 2011.

- **Consequences-related data:** The input for secondary economic impacts[27] can have a substantial effect on how MSRAM's output ranks a facility relative to other potential targets. Undervaluing secondary economic impacts could result in a lower relative risk ranking that underestimates the security risk to a facility, or inversely, overvaluing secondary economic impacts could result in overestimating the security risk to a facility. However, the Coast Guard has limited data for assessing secondary economic impacts from an attack on OCS facilities or deepwater ports. Coast Guard analysts stated that gathering these data is a challenge because there are few models or guidance available for doing so. During the course of our review, the Coast Guard started using a tool, called "IMPLAN," that helps inform judgments of secondary economic impacts by showing what the impact could be for different terrorist scenarios.[28] The tool, however, has limits in that it should not be used where the consequences of a terrorist attack are mainly interruption to land or water transportation. Enhancing DHS's and the Coast Guard's ability to assess secondary economic impacts could improve a MSRAM

[27]According to the Coast Guard, secondary economic impacts are a factor representing a description of follow-on economic effects of a successful attack.

[28]IMPLAN stands for IMpact Analysis for PLANning. It is a tool that assesses economic relationships between primary economic impacts and secondary economic impacts.

analyst's accuracy in assessing the relative risk of a particular target. Coast Guard officials added that they are working with DHS's Office of Risk Management and Analysis in studying ways to improve how it assesses secondary economic impacts.

Challenges in Scope

- **Challenges in assessing security risks to OCS facilities:** We determined that the Coast Guard did not conduct MSRAM assessments for all 50 of the OCS facilities that are subject to federal security requirements in 2011. Coast Guard guidance calls for MSRAM analysts to identify and assess all significant targets that fall within a unit's area of responsibility, which includes all security-regulated OCS facilities. Specifically, as of May 2011, we found that MSRAM did not include 12 of the 50 OCS facilities operating at that time. Coast Guard officials generally agreed with our finding and they have since incorporated these 12 facilities into MSRAM and completed the required risk assessments. While the Coast Guard plans to update its policies and procedures for inspecting and ensuring the security of OCS facilities in the future, the current set of policies and procedures do not call for an updated list of OCS facilities to be provided to MSRAM analysts to assess the security risks to such facilities annually. Coast Guard officials acknowledged that their policies and procedures did not include this requirement. Revising policies and procedures to include such a requirement is important in that the number of OCS facilities could change each year. For example, some facilities may drop below the production or personnel thresholds described earlier in this statement, thereby falling outside the scope of 33 C.F.R. part 106, or other facilities could meet or exceed such thresholds, thereby rendering them subject to part 106. *Standards for Internal Control in the Federal Government* state that policies and procedures enforce management directives and help ensure that actions are taken to address risks.[29] In addition, internal control standards state that such control activities are an integral part of an entity's planning, implementing, reviewing, and accountability for stewardship of government resources and for achieving effective results. Developing such procedures could help ensure that the Coast Guard carries out its risk assessment requirements for such security-regulated OCS facilities.

[29]GAO/AIMD-00-21.3.1.

- **Challenges in assessing security risks to offshore energy infrastructure that is not subject to security requirements:** With respect to OCS facilities, analysts only use MSRAM to assess security risks associated with those OCS facilities that are regulated for security under 33 C.F.R. part 106. For example, the *Deepwater Horizon* did not meet the threshold criteria subjecting it to regulation under part 106, and therefore, MSRAM was not used to assess its security risks (see fig. 2 for a photo of the *Deepwater Horizon* explosion). According to Coast Guard officials, mobile offshore drilling units (MODUs), such as the *Deepwater Horizon*, do not generally pose a risk of a terrorist attack since there is little chance of an oil spill when these units are drilling and have not struck oil.[30] However, the officials noted that there is a brief period of time when a drilling unit strikes a well, but the well has yet to be sealed prior to connecting it to a production facility. The *Deepwater Horizon* was in this stage when it resulted in such a large oil spill. During that period of time, MODUs could be at risk of a terrorist attack that could have significant consequences despite a facility not meeting the production or personnel thresholds. For example, such risks could involve the reliability of blowout preventer valves—specialized valves that prevent a well from spewing oil in the case of a blowout. Gaining a fuller understanding of the security risks associated with MODUs, such as the *Deepwater Horizon*, could improve the quality of program decisions made by Coast Guard managers on whether actions may be needed to ensure the security of this type of facility. According to Coast Guard officials, they are studying the "lessons learned" from the *Deepwater Horizon* incident and part of the study involves examining whether analysts should use MSRAM to assess MODUs in the future.

[30]MODUs engage in drilling rather than production.

Figure 2: Explosion of the *Deepwater Horizon* Drilling Unit in the Gulf of Mexico, April 2010

Source: U.S. Coast Guard.

- **Challenges in assessing systemic or network risks:** MSRAM does not assess systemic or network risks because, according to Coast Guard officials, these types of assessments are beyond the intended use of MSRAM. The 2009 National Infrastructure Protection Plan, 2010 DHS Quadrennial Review,[31] and a National Research Council evaluation of DHS risk assessment efforts[32] have determined that gaining a better understanding of network risks would help to understand multiplying consequences of a terrorist attack or simultaneous attacks on key facilities. Understanding "network" risks involves gaining a greater understanding of how a network is

[31]U.S. Department of Homeland Security: *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland* (Washington D.C.: February 2010).

[32]National Research Council: *Review of the Department of Homeland Security's Approach to Risk Analysis* (Washington D.C.: 2010).

vulnerable to a diverse range of threats. Examining how such vulnerabilities create strategic opportunities for intelligent adversaries with malevolent intent is central to this understanding. For example, knowing what damage a malicious adversary could achieve by exploiting weaknesses in an oil-distribution network offers opportunities for improving the resiliency of the network within a given budget.[33]

How the Coast Guard assesses offshore infrastructure within the broader set of networks is important. The findings of the National Commission on the BP *Deepwater Horizon* Oil Spill incident illustrate how examining networks or systems from a safety or engineering perspective can bring greater knowledge of how single facilities intersect with broader systems.[34] The report noted that "complex systems almost always fail in complex ways" and cautioned that attempting to identify a single cause for the *Deepwater Horizon* incident would provide a dangerously incomplete picture of what happened. As a result, the report examined the *Deepwater Horizon* incident with an expansive view toward the role that industry and government sectors played in assessing vulnerabilities and the impact the incident had on economic, social, and environmental systems. Enhancing knowledge about the vulnerabilities of networks or systems with which OCS facilities and deepwater ports intersect could improve the quality of information that informs program and budget decisions on how to best ensure security and use scarce resources in a constrained fiscal environment. Doing so would also be consistent with DHS's Quadrennial Review and other DHS guidance and would provide information to decision makers that could minimize the likelihood of being unprepared for a potential attack. Coast Guard officials agreed that assessing "network effects" is a challenge and they are examining ways to meet this challenge. However, the Coast Guard's work is this area is in its infancy and there is uncertainty

[33]See Gerald G. Brown, W. Matthew Carlyle, Javier Salmerón, and Kevin Wood, Operations Research Department, Naval Postgraduate School: *Analyzing the Vulnerability of Critical Infrastructure to Attack and Planning Defenses* (Monterrey, California: 2005). According to DHS, resiliency is the ability to resist, absorb, recover from, or successfully adapt to adversity or a change in conditions.

[34]National Commission on the BP *Deepwater Horizon* Oil Spill and Offshore Drilling, *Deep Water: The Gulf Oil Disaster and the Future of Offshore Drilling* (Washington D.C.: January 2011).

regarding the way in which the Coast Guard will move forward in measuring "network effects."

Conclusions

The threat of terrorism against energy tankers and offshore energy infrastructure highlights the importance of the Coast Guard having policies and procedures in place to better ensure the security of energy tankers, OCS facilities, and deepwater ports. The Coast Guard has taken steps to implement prior GAO recommendations to enhance energy tanker security, and it continues to work towards implementing the three outstanding recommendations. Improvements in security could help to prevent a terrorist attack against this infrastructure, which could have significant consequences, such as those resulting from the *Deepwater Horizon* incident. While the Coast Guard does not consider OCS facilities that it has assessed in MSRAM to be high risk, it is important to assess all OCS facilities as required by Coast Guard guidance. Since May 2011, when we determined that some OCS facilities were not assessed, the Coast Guard has completed its assessments for the previously omitted facilities. However, given that the list of security-regulated facilities may change each year based on factors such as production volume, it is important to ensure that any facilities added to the list in the future will be assessed for security risks in MSRAM. By revising policies and procedures to help ensure that an updated list of OCS facilities is provided to MSRAM analysts on an annual basis, the Coast Guard would be better positioned to ensure that all risk assessments for facilities requiring such assessments be conducted in a manner consistent with the law and presidential directive.

Recommendations for Executive Action

To strengthen the Coast Guard's efforts to assess security risks and ensure the security of OCS facilities, we recommend that the Commandant of the Coast Guard revise policies and procedures to ensure that MSRAM analysts receive the annual updated list of security-regulated OCS facilities to ensure that risk assessments have been conducted on all such OCS facilities.

Agency Comments and Our Evaluation

We provided a draft of this testimony to DHS and DOJ for comment. The Coast Guard concurred with our recommendation to revise policies and procedures to ensure that MSRAM analysts receive the annual updated list of security-regulated OCS facilities. DHS and DOJ provided oral and technical comments, which we incorporated as appropriate.

Chairman McCaul, Ranking Member Keating, and Members of the Subcommittee, this concludes my prepared statement. This testimony concludes our work on Coast Guard efforts to assess security risks for offshore energy infrastructure. However, we will continue our broader work looking at the security of offshore energy infrastructure, including Coast Guard security inspections and other challenges. Our evaluation will focus on Coast Guard security inspections and other measures to better secure OCS facilities and deepwater ports.[35] We will continue to work with the Coast Guard to develop solutions to ensure that inspections of OCS facilities are completed as required.

I would be happy to respond to any questions you may have.

[35]We are conducting this work for the Chairman of the Senate Committee on Commerce, Science, and Transportation; the Ranking Member of the Senate Committee of Homeland Security and Governmental Affairs; the House Committee on Energy and Commerce; the Chairman of the House Committee on Transportation and Infrastructure; the Ranking Member of the House Committee on Homeland Security; and the Ranking Member of the House Committee on Natural Resources; and the Chairman of the House Homeland Security Committee's Subcommittee on Oversight, Investigations, and Management.

GAO Contact and Staff Acknowledgments

Key contributors to this testimony were Christopher Conrad, Assistant Director; Neil Asaba, Analyst-in-Charge; Alana Finley; Christine Kehr; Colleen McEnearney; Erin O'Brien; Jodie Sandel; and Suzanne Wren. Chuck Bausell contributed economics expertise, Pamela Davidson assisted with design and methodology, Tom Lombardi provided legal support, and Jessica Orr provided assistance in testimony preparation.

Related GAO Products

Maritime Security: Updating U.S. Counterpiracy Action Plan Gains Urgency as Piracy Escalates off the Horn of Africa. GAO-11-449T. Washington, D.C.: March 15, 2011.

Quadrennial Homeland Security Review: 2010 Reports Addressed Many Required Elements, but Budget Planning Not Yet Completed. GAO-11-153R. Washington, D.C.: December 16, 2010.

Maritime Security: DHS Progress and Challenges in Key Areas of Port Security. GAO-10-940T. Washington, D.C.: July 21, 2010.

Maritime Security: Actions Needed to Assess and Update Plan And Enhance Collaboration among Partners Involved in Countering Piracy off the Horn of Africa. GAO-10-856. Washington, D.C.: September 24, 2010.

Critical Infrastructure Protection: Update to National Infrastructure Protection Plan Includes Increased Emphasis on Risk Management and Resilience. GAO-10-296. Washington, D.C.: March 5, 2010.

Maritime Security: Federal Efforts Needed to Address Challenges in Preventing and Responding to Terrorist Attacks on Energy Commodity Tankers. GAO-08-141. Washington, D.C.: December 10, 2007.

Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure. GAO-06-91. Washington, D.C.: December 15, 2005.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548